International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 1, Feb 2014, 35-42
© TJPRC Pvt. Ltd.

A NOVEL APPROACH FOR FAKE ACCESS POINT DETECTION AND PREVENTION IN WIRELESS NETWORK

SANDIP S. THITE[1], SANDEEP VANJALE[2] & P. B. MANE[3]

[1,2]Department of Computer, BVDUCOE, Pune, Maharastra, India

[3]Department. of Electronics, AISSMS, Pune Maharastra, India

ABSTRACT

Currently many organizations utilize the wireless LAN to provide the access channel to the Internet and Intranet enabling the flexible workforce. While doing so, communications with the Internet is continuously maintained. The growing acceptance of wireless network causes a risk of wireless security attack. However the wireless security is always a primary concern. So for securing data in WLAN it is necessary to detect unauthorized access points which are installed without explicit authorization from a local network management. Rogue APs potentially open up the network to unauthorized parties, who may utilize the resources of the network, steal sensitive information or even launch attacks to the network. This has forced the issue to develop systems that will not only detect the unauthorized access points but also detect network attacks performed by authorized or unauthorized access points so that it protects data from external misuse. In network attacks, the hackers try to break the security of the network, by affecting host and then proceeding towards further damage. Due to the above security and performance threats, detecting unauthorized APs as well as detecting attacks performed by unauthorized or authorized AP'S is one of the most important tasks for a network manager.

KEYWORDS: Wireless Security, Fake Access Point, RSSI, 802.11

INTRODUCTION

The increase in the number of WI-FI users in the world has been impressive. Many public places provides a Wi-Fi connectivity with free of cost. All the Wi-Fi devices are connected to wireless network through a device called as the wireless access point (WAP). The access point is very popular because of features like it is scalable , cost effective, easy to install, easy to configure and most importantly it provides mobility.

Airtight report [1] shows that lack of knowledge about secure wireless network causes number of security threats. Malicious AP is one of the security threats in a wireless network. Malicious Aps are easy to deployed, hard to detect and open enterprise networks to a variety of attacks. The most common active attacks are Denial of Service, Man-in-the Middle attack. There are a number of existing techniques are available for the purpose of detection of malicious AP. The previous work contained several limitations. In server side approach if the client is far away from the server then server can't give the guarantee about security of client node. Even if the server not learnt about the wireless environment even after that it cannot detect the malicious AP. Existing malicious AP detection method only made for network administrator. These solutions are expensive, limited and not consider many cases.

To address the shortcomings of existing solutions we have proposed fake access point prevention system (FAPPS). This uses the Service Set Identifier (SSID), MAC address and received signal strength. By analyzing these attributes of the frame we can decide that the given access point is authorized one or not.

Our Main Contribution is as Follows

- We examined and analyzed different types of techniques to detect unauthorized access points.
- We proposed an approach called as FAPPS which works efficiently for detection and prevention of the access point.
- We implemented a prototype of our approach and evaluated it by creating several unauthorized access points in our wireless network. Our results shows that our proposed solution is not only detect but also prevent these APs from access.

BACKGROUND

The malicious access point is divided into two categories

Fake Access Point: It is created or installed by malicious attacker which is not part of the network. Without knowing to authorize user it performs attacks like man-in-the-middle attack, denial of service attack. It is set up by a malicious attacker for the purpose of malicious behavior such as falsification, eavesdropping, steals the information.

Rogue Access Point: the term rouge AP has been used in more than one context in wireless security literature. It is installed or set by not only by the outside attacker but also authorized user on the network to take a more advantages of the network.

It is very easy to create a fake AP. As shown in the figure, attacker configures his access point by using some software available in the market. After creating a fake AP attacker wait for a client node to connect to that fake AP or sometimes actively send multiple signals to client node and force him to change the connection. Even it analyzes the wireless traffic using tools like Aircrack-ng suite [11]. It captures the beacon and management frame and try to get nodes MAC address Logical address and Service set Identifier (SSID). By this way it performs attack on client nodes. Without creating an additional network connection it uses the internet services for wired network through authorized AP and provides it to client node. By this way an attacker steal the personal information of client node without knowing the client.

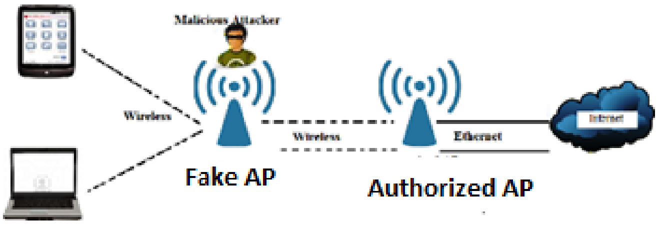

Figure 1: An Example of Fake AP Attack

RELATED WORK

There are a number of fake AP detection techniques. Traditional approach uses the concept of MAC Address checking, wireless traffic analysis for the detection of fake access point. But now a day's attacker can easily overcome these challenges of traditional approaches. In market there is no. of software tools available which are used in network for detection of fake AP. e.g. Airtights WIPS, Aerohived. Air Defense [2] provide a complete software & hardware system which contain sensors deploy throughout the network. Management console provided to network manager to handle the tool. Starter kit provides five sensors which manage upto ten APs. It detects intruders and attacks and also detects vulnerabilities in the network. The drawback of this tool is response time is very slow in order to detect the fake AP. It is a commercial product.

Air Magnet [3] is another commercial product which is used for detection of vulnerabilities and intrusions. It detects unauthorized Aps and DoS attacks by flooding. But this software product requires a technical person to move around the network for detection of security threats.

Han et al. [4] proposed timing based scheme for unauthorized access point detection. It uses a client side approach where the emphasis on Round Trip Time (RTT) between the user and the DNS server to check whether the access point is unauthorized AP or not. The detection algorithm is effective and accurate but they only consider wireless traffic between the station and the tested access point and set the unauthorized access point. The tradeoff between the overhead and accuracy occurs a large overhead. They also not consider the case of multiple unauthorized AP colluding with each other. Kao et al. [5] Proposed client side rogue access point detection technique using bottleneck Bandwidth analysis. It uses a passive packet analysis approach. It is based on bandwidth estimation using packet pair technology. They also proposed another approach called as client side bottleneck bandwidth with sliding window to get better accuracy with detection technique. But this technique has a problem about how to reduce the size of the sliding window. Packet analysis requires a sophisticated algorithm design which can be quickly deployed to protect the entire network.

Kim et al. [6] Proposed client side approach using the concept of received signal strength (RSS) for fake AP. In this method they find highly correlated RSS sequences that can be collected in the wireless device. After that they normalized the received signal and classify whether the collected signal is multiple or not. For that they use a sequential hypothesis technique. It is a lightweight solution to overcome the drawbacks of the client side approach. But in this technique they never consider a distance between the client node and access points while calculating the signal strength. Distance affects the signal strength.

Chao Yang et al. [7] proposed client side evil twin detection technique. This technique presents two algorithms: Training Mean Matching (TMM) and Hop Differentiating Technique (HDT). These algorithms use Inter-packet Arrival Time (IAT) to detect Evil Twin AP. This technique does not need authorized AP List and it is also not rely on training data or types of wireless network. The major problem with this technique is that it cannot work for all kinds of man-in-the-middle attacks in wireless networks. If remote servers are not available then this technique may not work correctly.

PROBLEM DEFINATION

In this section, we describe fake access point detection model with its learning mode and detection mode. The problems we resolve to detect with regard to fake Aps are twofold.

- Detection of fake AP without assistance from a network manager and without extra device.
- Analyze the signal strength to get a maximum bandwidth.

DESIGN

In this section we will explain our problem statement and our approach towards solving the problem. Our first priority is that our solution must work on any network which include wired, wireless and heterogeneous network. While designing a system we work in two modes, Learning and detection mode. Using this we can create an authorized access point list in a particular network. We provide this authorized list as an input to the detection module. We analyze the network and by using MAC address, SSID and RSSI we can decide whether detected AP is authorized one or not.

Our Main Contributions Are As Follows

- We provide a light weight solution which accurately detects the fake AP with minimum delay.

- Our method can easily deploy on any network and detect fake AP without adding any extra monitoring device in the network.
- Our method does not require any modification of the AP device.
- It can detect the fake APs even if the traffic is encrypted.

Apart from detection of fake AP, it helps the network administrator to maintain the authorized Access point list. And also provides the signal strength information which is useful for user to connect to AP for proper utilization of AP with nodes.

FAKE ACCESS POINT DETECTION MECHANISM

Fake access point detection mechanism works in two modes.

- First mode which is used to create an authorized access point list is called as learning mode.
- The second mode is used for detection of fake access point within a network this mode is called as Detection mode.

We select two modes, a) Learning Mode b) Detection mode

- **Learning Mode:** learning mode is used to create a whitelist, basically called as authorized AP list. Network administrator used this mode to maintain all authorized AP list. We called it as a Whitelist. Whitelist contain details about access point. Which includes MAC address, SSID and RSSI (Received Signal Strength Indicator). An updated whitelist is used as an input for detection mode. Initially we can start our system in learning mode considering all available AP are authorized AP. And collect information about all AP's available in network.
- **Detection Mode:** In detection mode, Initially it checks for the SSID, If the system finds any duplicate SSID or two AP's having the same SSID then it search for MAC address of these two AP's. If it finds the MAC address same then it considers it as authorized AP but it has a duplicate entry in it. But it found that if it has a different MAC address then it check its RSSI. If RSSI value is same as in whitelist or it is less than or greater than original value and the difference is +10 to -10 then we consider it as authorized AP else it generate warning message, then network administrator take an action against that particular AP by using Prevention policy.

SYSTEM ARCHITECTURE

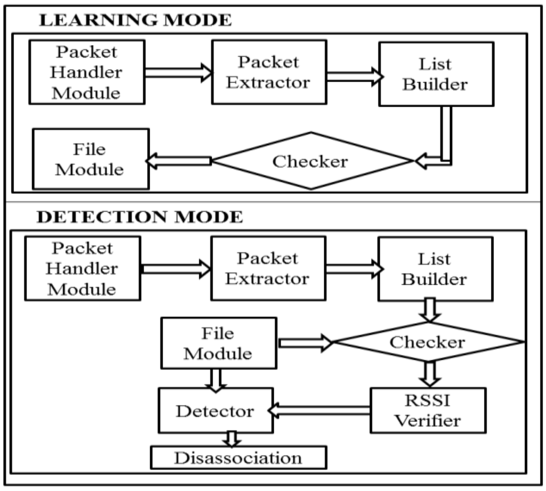

Figure 2: System Architecture

- **Packet Handler Module:** It is used to capture a beacon and management frame in a wireless network.
- **Packet Extractor:** It is used to extract the information from captured frame, where the information includes SSID, MAC address and received signal strength of the AP.
- **List Builder:** It is used to create a list of access points in network with detailed information. It is used for creation of whitelist which is also called as a Legitimate AP list.
- **Checker:** It is used to check duplicate Aps.
- **File Module:** It contains Whitelist. I.e. authorized AP list.
- **RSSI Verifier:** It verifies received signal strength value.
- **Detector:** It detects the fake AP in the network.
- **Disassociation:** It is used for the prevention of fake AP. i.e. unauthorized AP blocking.

Algorithm

```
Input – Beacon or Management frame.
Output – Authorized AP list and Unauthorized AP list.
Begin
        Select mode
                If mode =0 then
                Implement learning mode step 1.
                If mode =1 then
                Detection mode go to step 2.
        Step 1 : Mode =0
                Then Capture beacon and management frame
                Analyze frame & Extract packet header
                Read SSID, MAC address, RSSI.
                Generate Authorized AP list.
        Step 2 : Mode =1
                 Then Capture beacon and management frame
                Analyze frame & Extract packet header
                Read SSID, MAC address, RSSI.
                If (Two AP = Same SSID)
                Then Check MAC address of these two AP
                IF (To AP = Same MAC address)
```

```
            Then end
            Else check (Two AP = same RSSI level or ±10)
            Then AP = Authorized AP
            Else Fake AP
End.
```

IMPLEMENTATION

We implement our method in Python. We used airmon-ng of aircrack suite [11] for capturing wireless traffic. The Airmon - ng is useful even we want to capture encrypted wireless traffic. We used scapy library of python for the purpose of capturing and handling packets. We initially capture beacon and management frame in a wireless network. Some AP block's beacon frame so here we also consider a management frame. Packet extractor is used to extract captured packet and read the information from different fields of the packet. After executing this step we get detailed information of each access point. In learning mode we create a one file called as whitelist file and in that file we stored authorized AP’s by its MAC address, SSID and RSSI of AP.

In detection mode it captures the beacon and management frame of each AP available in the network and it gets SSID, MAC address and RSSI from list builder. Initially it verifies the SSID from the list. If it Found more than one AP has same SSID, i.e. two AP has the same SSID then it checks to MAC address of these Two AP’s. If it found the same MAC address then it consider as a repeated entry of same AP. But if it found that it has different MAC address than whitelist then it checks it RSSI. Here we can use a received signal strength indicator (RSSI) for the detection of fake AP. We take an RSSI level in between -100 and 0. Where 0 means the device was exactly at the place of detector and -100 means it is very far away. For example if for one access point we have an RSSI value -40 in our whitelist. But it shows the value around -50, even after that we consider it as an authorized AP. And if it shows value like -90. It means that there is a chance of fake AP present in the network. We will consider ±10 in RSSI level. But if the new RSSI value shows a big difference to the value present in the whitelist then system generate a warning message about that particular AP. So after detecting fake AP we implement prevented or blocking policy on that AP. So we perform disassociation with that particular node

MATHEMATICAL MODEL

Let set A ={a1,a2,a3,…,an}

Set A contain subset a1 ={si,mi,ri};

Consider mode value = 0

$$\mathbf{W(L)}=\boldsymbol{f(L)} = \sum_{n}^{0} \mathbf{P(a1)} + \sum_{n}^{0} \mathbf{P(ai)}$$

Consider mode value = 1

$$\mathbf{D(L)}=\boldsymbol{f(L)} = \sum_{n}^{0} \mathbf{P(a1)} + \sum_{n}^{0} \mathbf{P(ai)}$$

But if W(L) ≠D(L)

Then We can check value attributes

W(L) {ai(si, mi, ri) } ≠ D(L) {ai(si, mi, ri) }

Then

D(L)⊄ W(L)

Results of Our Solution

This software is being tested in a college network, where it generates a white list and also detects the fake AP in a network by sending a warning message.

It initially createsan authorized AP list

Learning Mode

Table 1

Sr. No.	SSID	MAC Address	RSSI
1	AndroidAP	00:02:6f:5f:39:a3	-94
2	SST	20:10:7a:39:db:39	-78
3	BVCOEW	f8:1a:67:a1:06:cd	-93
4	Nano-con	bc:79:ad:52:81:ae	-40
5	IDEA-GPRS	00:7a:39:db:39:f8	-39
6	BVOCEP	52:81:5f:39: 06:cd	-52
7	BVG	06:cd:ad:52:6f:5f	-49

Detection Mode

Table 2

Sr. No.	SSID	MAC Address	RSSI
1	**AndroidAP**	**00:02:6f:5f:39:a3**	**-94**
2	SST	20:10:7a:39:db:39	-78
3	BVCOEW	f8:1a:67:a1:06:cd	-93
4	Nano-con	bc:79:ad:52:81:ae	-40
5	**AndroidAP**	**00:02:6f:5f:39:a3**	**-22**
6	IDEA-GPRS	00:7a:39:db:39:f8	-39
7	BVOCEP	52:81:5f:39: 06:cd	-52
8	BVG	06:cd:ad:52:6f:5f	-49

In detection mode we found Access point with same SSID, MAC Address but the RSSI level is different. From this comparisons we can block access point AndroidAP with RSSI = -22.

EVALUATION

To measure the effectiveness of our approach, initially we run our software in trusted wireless network. We get a whitelist within a 1 millisecond. After that we injected a fake access point in our wireless network. We ran our software in wireless networks for detection mode. And within a fraction of seconds we get warning message about fake AP in the network with its SSID, MAC address, RSSI. We provide a lightweight solution which accurately detects the fake AP with minimum delay. Without adding any extra monitoring device in the network. Even our method does not modify the existing setup. It can detect the fake APs even if the wireless traffic is encrypted.

LIMITATION AND FUTURE SCOPE

Our current approach efficiently detects the fake access point. But environmental condition can affect the RSSI and also mobility of Smartphone AP causes a drastic change in value of RSSI. In this scenario it is quite difficult to find a fake AP in the network. In future scope, by using an RSSI level we can find the approximate distance in between access point and client node.

CONCLUSIONS

The fake access point detection system has been a major research area because of increased use of wireless network. In this paper we have presented a fake AP detection method with its merits and demerits. This method considers different but important parameters like SSID, MAC address and RSSI. It also captures encrypted traffic data to analyze the network. This method overcomes the drawbacks of existing techniques. Our experimental results show that our solution is cost effective, scalable, and easily deployable on any network. It is a lightweight solution without modifying network architecture.

REFERENCES

1. AirTight Network. Available: http://www.airtightnetwork.com
2. Airdefense enterprise: WIPS. Available: http://www.airdefense.net
3. Airmagnet. Available: http://www.airmagnet.com
4. H. Han, B. Sheng, C. Tan, Q. Li,and S. Lu "A Measurement based rogue access point detection scheme," in INFOCOM,2009, pp.1593-1601.
5. K. kao, I-En Liao, Y-C Li, " Detecting rogue access points using client-side bottleneck bandwidth analysis," ScienceDirect, computers & security 28 (2009),144-152
6. T. Kim, H. Park, H.Jung and H. Lee(2012) "Online detection of fake access points using received signal strength"
7. C. Yang, Y. Song and G. Gu, "Active user-side evil twin access point detection using statistical techniques"
8. G. Shivraj, M. Song and S. Shetty, "A hidden markov model based approach to detect rogue access points" IEEE, 978-1-4233-2677,2008.
9. B. Yan, G. Chen, J. Wang, and H. Yin, "Robust detection of unauthorized wireless access points," Springer, Mobile Network Appl (2009),508-522.
10. W. Wei, K. Suh, B. Wang. J. Kurose and D. Towsley, " Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs. In Proc. 7th ACM SIGCOMM conference on Internet measurement, (2007).
11. Aircrack. http://www.aircrack-ng.org